Norms in Q(alpha)[x]

November 21, 2023 8:46 AM

Def. Let $m(z) \in \mathbb{Q}[z]$ be the min. poly. for $\alpha \in \underline{\mathbb{C}}$.

Since $m(\alpha) = 0 \Rightarrow m(z) = (z - \overset{\alpha_1}{\overset{\shortparallel}{\alpha}})(z - \alpha_2) \cdot \cdots \cdot (z - \alpha_d) = 1 \cdot z^d + \cdots$

Let $a(\alpha) \in \mathbb{Q}[\alpha]$. Define the <u>norm of $a(\alpha)$</u> by

$$N(a(\alpha)) = a(\alpha) \cdot a(\alpha_2) \cdot \cdots \cdot a(\alpha_d).$$

E.g. $\alpha = \sqrt{2}$. $m(z) = z^2 - 2 = (z - \sqrt{2}) \cdot (z - (-\sqrt{2}))$

Let $a(\alpha) = 1 + 2\alpha$. $N(a) = (1 + 2\sqrt{2})(1 - 2\sqrt{2}) = 1 - 8 = -7 \in \mathbb{Q}$.

Recall $\operatorname{res}(A(x), B(x)) = a_m^{\overset{\deg(B)}{\overset{\shortparallel}{n}}} \prod_{i=1}^{m} B(\underbrace{\alpha_i}_{\uparrow \text{roots of } A.})$ where $A = a_m \prod_{i=1}^{m} x - \alpha_i$

Observe $\operatorname{res}(\underset{\uparrow}{m(z)}, a(z)) = 1 \prod_{i=1}^{d} a(\alpha_i) = N(a(\alpha))$.   roots of $m(z)$.

But. $\operatorname{res}(\underset{\mathbb{Q}[z]}{\underset{\Uparrow}{m(z)}}, \underset{\mathbb{Q}[z]}{\underset{\Uparrow}{a(z)}}, z) \in \mathbb{Q} \Rightarrow N : \mathbb{Q}[\alpha] \to \mathbb{Q}$.

Main property of the norm N: given $a(\alpha), b(\alpha) \in \mathbb{Q}[\alpha]$

$$N(a \cdot b) = \operatorname{res}(m(z), a(z) \cdot b(z)) = \operatorname{res}(m, a) \cdot \operatorname{res}(m, b)$$
$$= \overset{\shortparallel}{N}(a) \cdot N(b).$$

<u>Norms in $\mathbb{Q}(\alpha)[x]$.</u>

Let $f(x, \alpha) \in \mathbb{Q}(\alpha)[x]$, $\deg(f, x) \geq 0$ and $m(z)$ is the min. poly. for α. $m(z) = \prod_{i=1}^{d} (z - \alpha_i)$.

Define

$$N(f(x, \alpha)) = f(x, \overset{\alpha_1}{\overset{\shortparallel}{\alpha}}) \cdot f(x, \alpha_2) \cdot \cdots \cdot f(x, \alpha_d)$$
$$= \operatorname{res}(\underset{\mathbb{Q}[z]}{\underset{\Uparrow}{m(z)}}, \underset{\mathbb{Q}[x][z]}{\underset{\Uparrow}{f(x, z)}}, z) \in \mathbb{Q}[x].$$

Ex. $\alpha = \sqrt{2}$

$m = z^2 - 2.$

$f(x,\alpha) = 1 + \alpha \cdot x$

$f(x,z) = 1 + zx$

$N(f(x,\alpha)) = f(x,\sqrt{2}) \cdot f(x,-\sqrt{2})$

$= (1+\sqrt{2}x)(1-\sqrt{2}x)$

$= 1 - 2x^2 \in \mathbb{Q}[x].$

$res(m, f(x,z), z) = res(z^2-2, 1+zx, z)$

$$= \det\left(\begin{bmatrix} 1 & x & 0 \\ 0 & 1 & x \\ -2 & 0 & 1 \end{bmatrix}\right) = 1 - 2x^2.$$

Lemma 1 Properties of $N(f(x,\alpha))$.

irreducible.

$\gcd(m,f) \neq 1.$

(i) $N(f(x,\alpha)) = 0 \Longleftrightarrow res(m(z), f(x,z)) = 0 \Leftarrow m(z) \mid f(x,z).$

$\underset{m(\alpha)=0}{\Rightarrow} (z-\alpha) \mid f(x,z) \Rightarrow f(x,\alpha) = 0 \Rightarrow N(f(x,\alpha)) = 0.$

(ii) $N(f(x,\alpha) \cdot g(x,\alpha)) = (f) \cdot N(g).$

(iii) $0 \neq f(x,\alpha) \mid N(f(x,\alpha)) = f(x,\alpha) \underbrace{f(x,\alpha_2) \cdots\cdots f(x,\alpha_d)}$

(iv) $0 = f(x,\alpha) \mid g(x,\alpha) \Rightarrow N(f) \mid N(g).$

$f \mid g \Rightarrow g = fq \Rightarrow N(g) = N(fq) = N(f) \cdot N(q).$

$\Rightarrow N(f) \mid N(g).$

(v). $\deg(N(f(x,\alpha)), x) = \deg(m,z) \cdot \deg(f(x,\alpha), x).$